UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,793	04/13/2001	Jung-Wan Ko	1293.1191	1932

49455 7590 04/12/2005

STEIN, MCEWEN & BUI, LLP
1400 EYE STREET, NW
SUITE 300
WASHINGTON, DC 20005

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 04/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/833,793	KO ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-11,13-35,and 41-45* is/are pending in the application.

4a) Of the above claim(s) *2,12 and 36-40* is/are withdrawn from consideration.

5)☒ Claim(s) *1,3-6,8-9,13-5,17 and 31-33* is/are allowed.

6)☒ Claim(s) *18-30,34,35 and 41-45* is/are rejected.

7)☒ Claim(s) *7,10,11 and 16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *4/13/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1, 13, 17, 18, 29, 35, and 41 have been amended. Claims 2, 12, and 36-40 have been cancelled. Claims 1, 3-11, 13-35, and 41-45 are still pending. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

The examiner has considered the applicant's amendments. The examiner withdraws the previous 112, second paragraph rejections in light of the applicant's amendments and arguments.

Response to Arguments

Applicant's arguments filed on 3/15/2005 with respect to claims 18-35 have been considered and are persuasive but are moot in view of the new ground(s) of rejection.

In the submitted arguments on 3/15/2005, the examiner notes that the applicant did not argue against the reference used, Spelman et al (US 5,761,311), teaching the *encryption* limitations recited in the claims. For example:

- Encrypting a first region of a text containing a second encryption key using a first encryption key.
- Encrypting a second region of text using the second encryption key.
- Transmitting a cipher text comprising the encrypted first and second regions.

As such, the examiner assumes that the applicant agrees that it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made

to have used the *encryption* scheme as recited in the claims and that one of ordinary skill would have done so for the motivations given in the previous office action.

The examiner also notes that the applicant did not argue against any of the rejections of the limitations recited in the dependent claims as being improper using the references and reasoning applied. As such, the examiner assumes that the applicant agrees that the rejection of the limitations recited in the dependent claims are proper, excluding the limitations inherited from the independent claims of course.

Claim Objections

Claim 7, 10, 11, and 16 objected to because of the following informalities: claim 7, 10, 11, and 16 each depend on claim 2, which have been cancelled. The examiner assumes the applicant mean claim 1 instead of 2.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 18, 22-23, 30, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (US 5,761,311) in view of Orrin (US 6,011,849).

Claim 18:

Spelman discloses a computer readable medium encoded with processing instructions for implementing a method of encrypting a text sent between a sender and a receiver performed by a computer, the method comprising:

1. Encrypting a first region of the text using a first encryption key, where the first region contains a second encryption key (col 1, lines 42-56).
2. Encrypting a second region of the text using the second encryption key (col 1, lines 42-56).

Spelman does not explicitly disclose:

1. Decrypting the first region of the text using the first encryption key.
2. Extracting the second encryption key from the decrypted first region.
3. Decrypting the second region of the text using the extracted second encryption key.

However, Orrin discloses that the decryption is generally the equivalent of an encryption operation in reverse (col 9, lines 34-36). It was established in the last office action that the encryption method disclosed by Spelman was more complicated that the encryption method recited by the applicant. However, it was also established that Spelman still taught the above recited encryption method and one of ordinary skill would have been motivated to use the less complicated version as the more complicated version is not always needed, depending on how strong an encryption one wants. As such, it would have been obvious to one of ordinary skill in the art at the time the

applicant's invention was made that if a text was encrypted using the encryption method recited in claim 18, to decrypt the text, one must use the decryption method as recited above it is the reverse of the encryption process. One of ordinary skill would have been motivated to do so in light of common decryption process as disclosed by Orrin (col 9, lines 34-36). Note that to extract the second key, the receiver must also have information related to the second key.

Claim 22:

Spelman does not disclose the computer readable medium of claim 18, wherein the second encryption key is smaller than the first encryption key. However, one of ordinary skill would recognize that as the first encryption key is being used to protect the second encryption key, the second one does not have to be as large as the first. A smaller second key would allow for faster encryption of the bulk of the message. In this manner, a compromise between security and encryption speed can be reached.

Claim 23:

Spelman and Orrin do not disclose the size of the first encryption key is fixed, and the size of the second encryption key is varied by a transmission unit within the first region. However, one of ordinary skill would be motivated to do so as by fixing the size of the first encryption key, that information would not have to be transmitted to a receiving party via secure channel more than once if the receiving party was expected to receive multiple encrypted messages using the same encrypting method. This would save on the amount of network resources used by the system. By varying the size of the second encryption key by a transmission unit within the first region, one of ordinary

skill would make the second key more secure, thus perhaps making up for the first encryption key not being as secure as its size is fixed.

Claim 30:

Spelman does not explicitly disclose a computer readable medium encoded with processing instructions for implementing a method of decrypting an encrypted text sent between a sender and a receiver performed by a computer, the method comprising:

1. Decrypting the first region of the encrypted text using a first encryption key, where the first region contains a second encryption key.
2. Decrypting a second region of the encrypted text using the second encryption key.

However, is has been established already that Spelman teaches:

1. Encrypting a first region of the text using a first encryption key, where the first region contains a second encryption key (col 1, lines 42-56).
2. Encrypting a second region of the text using the second encryption key (col 1, lines 42-56).

Orrin discloses that the decryption is generally the equivalent of an encryption operation in reverse (col 9, lines 34-36). The decryption method recited in claim 30 is the reverse operation of the encryption method that has been established as being taught by Spelman. It would have been obvious to one of ordinary skill in the art to use the decryption method as recited in claim 30 in light of Orrin's teachings. One of

ordinary skill in the art would have been motivated to do so for the same reason given in claim 18.

Claim 35:

Spelman does not explicitly disclose the computer readable medium according to claim 30, wherein a first region of the encrypted text is smaller than a second region of the encrypted text, and a size of the first encryption key is larger than a size of the second encryption key. However, one of ordinary skill would recognize that as the first encryption key is being used to keep the second key safe, its strength would need to be stronger than the second, therefore its size would need to be larger. Further, as speed is a concern in encryption also, since the second encryption key is smaller, encryption using it would be faster, so as the second part of the message is encrypted using the second encryption key, it would make sense to make the second part of the message larger as this would allow encryption of the entire message to go faster.

Claims 19, 24-29, and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (US 5,761,311) in view of Orrin (US 6,011,849) and further in view of Lynn et al (US 5,345,508).

Claim 19:

Spelman et al do not explicitly disclose sending the first encryption key and information related to the second encryption key through a safe transmission path. However, Orrin disclosed that decryption is generally the reverse of encryption (col 9,

lines 34-36). As the first key was used to encrypt the first part of the message, the receiver would need the first key to decrypt the first part. Also, as the second key was used to encrypt the second part of the message, one would need the information related to the second key so that one may obtain the second key to decrypt the second part. There is no other way around this using the encryption method of claim 18, so one must therefore send the first encryption key and information related to the second encryption key to the receiver.

Spelman et al also do not disclose that the message was transmitted using a safe transmission path. However, Lynn et al disclose the transmission of confidential information such as a secret key through the use of a secure channel (col 1, lines 31-37 and fig 1(a)). One of ordinary skill would recognize that it would do no good to encrypt a message and transmit how it was encrypted to an intended party if the method and key used for encryption were fall into the hands of a hacker, so one of ordinary skill would most likely use a secure channel when transmitting such information.

Claim 24:

Spelman does not explicitly disclose the information related to the second encryption key includes size and position information of the second encryption key. However, as mentioned already, an decryption process is often the reverse of the encryption process as disclosed by Orrin (col 9, lines 34-36), so one of ordinary skill would recognize that one would need to send to a party who will be decrypting a message the information related to the second encryption key including the size and position information of the second encryption key.

Claim 25:

Spelman does not explicitly disclose the position and size information of the second encryption key are fixed. However, one of ordinary skill would be motivated to keep the position and size information of the second encryption key fixed as then that information would only be needed to be transmitted to a decrypting party once. This would save on network resources in networks where speed is more important than greater security.

Claim 26:

Spelman does not explicitly disclose the position and size information of the second encryption key are varied. However, one of ordinary skill would be motivated to vary the size and position information of the second key as sometime greater security is more important than encryption speed or conserving uses of network resources.

Claim 27:

Spelman does not explicitly disclose the first region of the text is smaller than the second region of the text. However, one of ordinary skill in the art would be motivated to keep the first region of text smaller than the second region as the larger the region that must be encrypted with the first encryption key, the longer it would take to do the encryption. As the second encryption key is encrypted by a first encryption key, which one of ordinary skill would presumably choose to be stronger than the second encryption key, it would be faster to encrypt most of the message with the second encryption key than the first.

Claim 28:

Spelman does not explicitly disclose sending information on a starting address of the second region through the safe transmission path. However, it would be obvious to one of ordinary skill in the art at the time of the applicant's invention to send such information, as it would be needed to properly decrypt the message. Further, Lynn et al disclose that the use of a safe transmission path to transmit sensitive information was known at the time of the applicant's invention (col 1, lines 21-27 and fig 1(a)). One of ordinary skill would use the safe transmission path to transmit this needed information so that a hacker would not gain this information and more easily break the encryption.

Claim 29:

Spelman does not explicitly disclose sending a cipher text comprising the first and second portions through an unsafe transmission path and obtaining the safe transmission path through authentication operations. However, Lynn et al disclose in fig 1(a) a cipher text message being sent over a public or unsafe transmission path. As the message is already encoded, one of ordinary skill would be motivated to send through the unsafe path as it would probably be faster and cheaper to do so. Neither Spelman et al nor Lynn et al disclose that the safe transmission path is obtained via authentication operations, but the examiner would like to use official notice to note that obtaining a safe path via authentication operations was well known at the time of the applicant's invention. One of ordinary skill would be motivated to make use of authentication operations to obtain a safe path as it is a simple and quick way of obtaining the safe path.

Claim 41:

Spelman does not explicitly disclose a receiver for receiving encrypted text, comprising:

1. An authenticator to obtain a safe transmission path through which a first encryption key and information related to a second encryption key are received.
2. A decryptor to decrypt a portion of the encrypted text using the first encrypted key, to extract the second encryption key from the decrypted ported using the information related to the second encryption key, and to decrypt another portion of the encrypted text using the second encryption key.

However, as established in the last office action, an authenticator for obtaining a safe transmission path was known at the time the applicant's invention was made. They are usually used for verification purposes. Further, Lynn discloses the use of a safe transmission path to receive sensitive data such as an encryption key (col 1, lines 21-27 and fig 1(a)). One of ordinary skill would be motivated to use to obtain a safe transmission path through which a first encryption key and information related to a second encryption key are received because it would do no good to encrypt a text if the key to decrypt it falls into the hands of a hacker.

Lynn also does not disclose a decryptor to decrypt a portion of the encrypted text using the first encrypted key, to extract the second encryption key from the decrypted ported using the information related to the second encryption key, and to decrypt another portion of the encrypted text using the second encryption key. However, Orrin discloses that decryption is generally the equivalent of an encryption operation in

reverse (col 9, lines 34-36). The decryption method recited in claim 30 is the reverse operation of the encryption method that has been established as being taught by Spelman. It would have been obvious to one of ordinary skill in the art to use the decryption method as recited in claim 41 in light of Orrin's teachings. One of ordinary skill in the art would have been motivated to do so for the same reason given in claim 18.

Claim 42:

Spelman does not explicitly disclose the information related to the second encryption key comprises size and position information of the second encryption key and the encrypted text is sent/received through an unsafe transmission path. However, Lynn discloses an encrypted text being sent/received through an unsafe transmission path (col 1, lines 21-27 and fig 1(a)). One of ordinary skill might want to send through an unsafe transmission path as it would be faster to do so and the text is encrypted already, therefore secure. Lynn et al also do not disclose the information related to the second encryption key comprising size and position information of the second encryption key. However, the information must comprise the size and position information as these information are needed to decrypt the message properly.

Claim 43:

Spelman discloses the receiver comprises an information appliance (col 4, lines 47-54)

Claim 44:

Spelman discloses the receiver comprises a computer (col 4, lines 47-54).

Claim 45:

Spelman discloses the receiver comprises a server (col 4, lines 47-54).

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (U.S. 5,761,311) in view of Orrin (US 6,011,849) and Lynn et al (U.S. 5,345,508) and further in view of Ganesan et al (U.S. 5,588,061).

Claim 20:

Spelman discloses that his invention can be used with computers and computer readable mediums (col 4, lines 48-54). Spelman does not disclose the computer readable medium of claim 19, wherein the larger first encryption key comprises an encryption key that is 56 bits or more. However, Ganesan discloses the use of an encryption key that is 56 bits or larger in size (col 6, 1st paragraph). One of ordinary skill would be motivated to use an encryption key that is 56 bits or larger for the first key as this would allow for greater encryption strength for the first key.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (US 5,761,311) in view of Orrin (US 6,011,849) and Lynn et al (US 6,5345,508) and further in view of Seheidt et al (US 5,787,173).

Claim 21:

Spelman, Orrin, and Lynn do not disclose the first encryption key comprises a public/asymmetric key for use with a public/asymmetric key encryption method. However, Seheidt et al disclose that the use of public key encryption was well known by one of ordinary skill in the art at the time of the applicant's invention (col 3, lines 4-31). One of ordinary skill would be motivated to use public key encryption for the first encryption key, as public key encryption is inherently more secure than common encryption keys, though encryption with it takes longer. One of ordinary skill would use public encryption keys where concerns for security far outweigh concern about encryption speed. The fact that public key encryption is typically slow, though strong was disclosed by Spelman also (col 8, last paragraph and col 9, 1st paragraph). Spelman disclosed that there are instances when it is more appropriate to use either public key or common key encryption over the other depending if one wanted speedier performance or greater encryption strength. The examiner would like to note that public keys are also known as asymmetric keys.

Allowable Subject Matter

Claims 1, 3-11, 13-17, 31-33 contain allowable subject matter.

As per independent claim 1, the examiner was able to find art which reads on the encryption method recited in claim 1. However, the examiner was not able to find the following limitations:

1. Transmitting the first encryption key, **region segmentation information for segmenting the text into the first region and the second region**, and information related to the second encryption key through a safe transmission path.
2. Decrypting the first region of the transmitted cipher text using the transmitted first encryption key **and the transmitted region segmentation information**.

One prior art found by the examiner disclosed that the decryption process is generally the equivalent of an encryption operation in reverse. However, the prior art found by the examiner which reads on the encryption method recited in claim 1 not only divided the text into segments, it also divided the text into blocks of data which are then sent to a receiver. The decryption process which the prior art used differ from the one recited by the applicant in claim 1 in that there was no need to send the region segmentation information to the receiver or use this information in the decryption process as the sender already took care to divide the text into blocks in which a key could be used without having to worry about how much of the message can be decrypted by the key. The examiner could find no motivation in the prior art which would explain why one of ordinary skill would transmit the region segmentation information and use said region segmentation information in the decryption process. Any motivation the examiner could suggest was suggested already by the applicant.

A similar limitation is recited in independent claim 13. Claims 3-11 and 14-17 depend on claims 1 or 13. Claims 7, 10, 11, and 16 each contain minor informalities, but would be allowed if they were fixed.

As per claim 31, it also recites decryption using the region segmentation information and as such contain allowable subject matter. Claim 32 and 33 depend from claim 31.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Kato (US 6,381,331).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100